

FILED  
2018 AUG 30 PM 4:23  
CLERK U.S. DISTRICT COURT  
CENTRAL DISTRICT OF CALIF.  
LOS ANGELES

UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2018 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

ORİYOMI SADIQ ALOBA,  
aka "D Rwal Me Dontry,"  
aka "davisdan0007,"  
VICTOR ADEDAMOLA,  
aka "Legendowski,"  
RIDWAN ALAGBADA,  
aka "Mr. Hottie Hottie,"  
FNU LNU,  
aka "Ionicle,"  
ROBERT CHARLES NICHOLSON, III,  
aka "Million\$Menace,"

Defendants.

CR No. 18-0083 (A) -RGK

F I R S T  
S U P E R S E D I N G  
I N D I C T M E N T

[18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud and Attempted Wire Fraud; 18 U.S.C. § 1343: Wire Fraud; 18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)(i), (ii): Unauthorized Access to a Protected Computer to Obtain Information; 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I): Unauthorized Impairment of a Protected Computer; 18 U.S.C. § 1028A: Aggravated Identity Theft; 18 U.S.C. § 2(a): Aiding and Abetting]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

1. Phishing is the fraudulent practice of sending emails purporting to be from a reputable or familiar source, such as a financial institution, social media company, or internet service

1 provider, to victims in order to induce the victims to reveal  
2 sensitive information, such as: names, addresses, Social Security  
3 numbers, dates of birth, and mothers' maiden names (collectively,  
4 "PII"); email usernames and passwords (collectively, "email  
5 credentials"); and credit and debit card information, including  
6 account numbers, expiration dates, credit verification values, and  
7 online account login and password information (collectively, "credit  
8 card information"). In a typical phishing scheme, the phishing email  
9 contains a link to a website that purports to be a legitimate  
10 business website but is, in fact, operated by a computer attacker.  
11 The website prompts the victim to enter his or her PII, email  
12 credentials, and/or credit card information, which is then collected  
13 and delivered to an email account belonging to the computer attacker  
14 ("harvester email account").

15 2. A phishing kit is a collection of software tools designed  
16 to enable phishing attacks. Phishing kits typically include website  
17 development software that can be used to create phishing websites and  
18 spamming software that allows users to automate the process of mass  
19 mailing phishing emails. The email address for the harvester email  
20 account is usually encoded in the software that creates the phishing  
21 website so that the stolen PII, email credentials, and credit card  
22 information is automatically delivered to the harvester email account  
23 every time a victim inputs that information into the phishing  
24 website.

25 3. Mobile payment and digital wallet services ("digital  
26 wallets") allow users to make credit and debit card purchases at  
27 certain retail stores using a smartphone rather than a physical card.  
28 To use a digital wallet, a user must do the following:



1           a.     First, the user enters certain credit card information  
2 into a digital wallet application, such as Apple Pay or Android Pay.

3           b.     Then, in a process referred to as dual-factor or two-  
4 factor identification, the application offers the user multiple  
5 options for receiving a verification code with which the application  
6 confirms that the user is the true account holder. Verification code  
7 delivery options typically include: (1) sending an email to the  
8 account holder's email account; (2) sending a text message to the  
9 account holder's cell phone; or (3) making a call to the account  
10 holder's phone number.

11           c.     Once in possession of the verification code, the user  
12 inputs it into the digital wallet application. Once the code has  
13 been accepted, the user can make purchases with his or her  
14 smartphone.

15           4.     At all times relevant to this indictment:

16           a.     Realmangreat@gmail.com (the "Realmangreat Account")  
17 and yalobaz@yahoo.com (the "Yalobaz Account") were email accounts  
18 belonging to defendant ORİYOMI SADIQ ALOBA, also known as ("aka") "D  
19 Rwal Me Dontry," aka "davidan0007" ("ALOPA").

20           b.     Microsoft Corporation ("Microsoft"), located in  
21 Redmond, Washington, operated computers used by subscribers all over  
22 the world in interstate and foreign commerce and communications. One  
23 of the services that Microsoft provided to its customers was Office  
24 365, an internet- or "cloud"-based computing system in which customer  
25 computing, software, and data storage (including email data) were  
26 located and managed remotely on servers owned by Microsoft.

27           c.     The Los Angeles Superior Court ("LASC"), located in  
28 Los Angeles County, within the Central District of California, used

1 Office 365 to host its employee email accounts, which have the domain  
2 "lacourt.org." LASC employees accessed their email accounts using  
3 unique usernames and passwords.

4 d. Victims M.P., R.H., R.I., M.C., and P.N. were LASC  
5 employees.

6 e. Emails sent from LASC employee email accounts were  
7 transmitted through Microsoft servers located in California, Iowa,  
8 Virginia, Washington, and Wyoming, among other locations.

9 f. American Express processed all credit card charges  
10 made in the western United States by wire through a server in  
11 Phoenix, Arizona.

12 g. Bank of America, N.A. ("Bank of America") processed  
13 all credit card charges by wire through a server in Richardson,  
14 Texas.

COUNT ONE

[18 U.S.C. § 1349]

5. The Grand Jury realleges and incorporates herein by reference the Introductory Allegations and Definitions of this First Superseding Indictment, as though fully set forth herein.

I. OBJECTS OF THE CONSPIRACY

6. Beginning on a date unknown to the Grand Jury and continuing until on or about August 1, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALOBA, VICTOR ADEDAMOLA, aka "Legendowski" ("ADEDAMOLA"), RIDWAN ALAGBADA, aka "Mr. Hottie Hottie" ("ALAGBADA"), First Name Unknown ("FNU") Last Name Unknown ("LNU"), aka "Ionicle" ("Ionicle"), and ROBERT CHARLES NICHOLSON, III, aka "Million\$Menace" ("NICHOLSON"), together with others known and unknown to the Grand Jury, knowingly combined, conspired, and agreed with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

II. THE MANNER AND MEANS OF THE CONSPIRACY

7. The object of the conspiracy was carried out, and was to be carried out, in substance, as follows:

a. Defendants ADEDAMOLA, ALAGBADA, and Ionicle would make and obtain phishing kits. In particular:

i. Defendant ADEDAMOLA made and obtained a phishing kit (the "Office 365 phishing kit") designed to create a phishing website (the "Office 365 phishing website") that purported to be a website for Office 365 but was, in fact, a fraudulent website designed to collect victim email credentials and deliver them to the Realmangreat Account. The Office 365 phishing kit was also designed to send copies of an email (the "Office 365 phishing email") to



1 victims that purported to be a communication from Microsoft but was,  
2 in fact, a fraudulent email intended to lure victims to the Office  
3 365 phishing website.

4           ii. Defendant ALAGBADA made and obtained a phishing  
5 kit (the "Dropbox phishing kit") designed to create a phishing  
6 website (the "Dropbox phishing website") that purported to be a  
7 website for Dropbox Business but was, in fact, a fraudulent website  
8 designed to collect victim email credentials and deliver them to the  
9 Realmangreat Account. The Dropbox phishing kit was also designed to  
10 send copies of an email (the "Dropbox phishing email") to victims  
11 that purported to be a communication from Dropbox Business but that  
12 was, in fact, a fraudulent email intended to lure victims to the  
13 Dropbox phishing website.

14           iii. Defendant Ionicle made a phishing kit (the  
15 "American Express phishing kit") designed to create a phishing  
16 website (the "American Express phishing website") that purported to  
17 be a website for American Express but that was, in fact, a fraudulent  
18 website designed to collect victim email credentials and deliver them  
19 to the Realmangreat Account. The American Express phishing kit was  
20 also designed to send copies of an email (the "American Express  
21 phishing email") to victims that purported to be a communication from  
22 American Express but that was, in fact, a fraudulent email intended  
23 to lure victims to the American Express phishing website.

24           b. Defendants ADEDAMOLA, ALAGBADA, and Ionicle would  
25 provide phishing kits to defendant ALOBA.

26           c. Defendants ADEDAMOLA, ALAGBADA, and Ionicle would help  
27 defendant ALOBA use the phishing kits to obtain victim PII, email  
28

1 credentials, and credit card information and deliver it to the  
2 Realmangreat Account.

3 d. Defendant ALOBA would possess stolen victim PII, email  
4 credentials, and credit card information in the Realmangreat Account.

5 e. Defendant ALOBA would use stolen email credentials  
6 obtained by phishing to log into victim email accounts without  
7 authorization in order to:

8 i. send phishing emails and test emails to himself  
9 at the Yalobaz Account to test his access to the victims' email  
10 accounts; and

11 ii. send phishing emails to other victims.

12 f. Defendant ALOBA would provide defendant NICHOLSON, and  
13 others known and unknown to the Grand Jury, with victim PII and  
14 credit card information obtained by phishing.

15 g. Defendants ALOBA and NICHOLSON would add victim credit  
16 card information to digital wallets without authorization, as  
17 follows:

18 i. Defendant NICHOLSON would input the victim credit  
19 card information into a digital wallet application;

20 ii. At defendant ALOBA's direction, defendant  
21 NICHOLSON would select the option to receive the verification code by  
22 email;

23 iii. Defendant ALOBA would log into the victim email  
24 account without authorization, obtain the verification code, and  
25 provide it to defendant NICHOLSON; and

26 iv. Defendant NICHOLSON would input the verification  
27 code into the digital wallet application.

1 h. Defendant NICHOLSON would use and attempt to use the  
2 digital wallet containing victims' credit card information to  
3 purchase and attempt to purchase goods at retail stores that he would  
4 later sell and remit a portion of the proceeds to defendant ALOBA.

5 III. OVERT ACTS

6 8. In furtherance of the conspiracy and to accomplish its  
7 objects, defendants ALOBA, ADEDAMOLA, ALAGBADA, Ionicle, and  
8 NICHOLSON, together with other co-conspirators known and unknown to  
9 the Grand Jury, on or about the dates set forth below, committed and  
10 willfully caused others to commit the following overt acts, among  
11 others, within the Central District of California and elsewhere:

12 A. April 30, 2017 - Unauthorized Use of Victim M.M.'s American  
13 Express Credit Card (Defendants ALOBA and NICHOLSON)

14 Overt Act No. 1: On or about April 30, 2017, by instant  
15 message, defendant NICHOLSON told defendant ALOBA that he was in  
16 California and "ready to go."

17 Overt Act No. 2: On or about April 30, 2017, by instant  
18 message, defendant ALOBA told defendant NICHOLSON that he had a  
19 credit card for defendant NICHOLSON to add to his digital wallet.

20 Overt Act No. 3: On or about April 30, 2017, by instant  
21 message, defendant ALOBA provided defendant NICHOLSON with victim  
22 M.M.'s name and address, and credit card information for M.M.'s  
23 American Express credit card ending in 6000 (the "M.M. American  
24 Express card").

25 Overt Act No. 4: On or about April 30, 2017, by instant  
26 message, defendant NICHOLSON sent defendant ALOBA a photo of a  
27 Samsung phone on whose screen was displayed options for receiving a  
28 digital wallet verification code.



1        Overt Act No. 5:        On or about April 30, 2017, by instant  
2 message, defendant ALOBA told defendant NICHOLSON to choose the email  
3 option.

4        Overt Act No. 6:        On or about April 30, 2017, by instant  
5 message, defendant ALOBA told defendant NICHOLSON that he had not  
6 received the verification code and told defendant NICHOLSON to use a  
7 different phone.

8        Overt Act No. 7:        On or about April 30, 2017, by instant  
9 message, defendant NICHOLSON told defendant ALOBA that he had a new  
10 phone.

11       Overt Act No. 8:        On or about April 30, 2017, by instant  
12 message, defendant ALOBA sent defendant NICHOLSON a verification  
13 code.

14       Overt Act No. 9:        On or about April 30, 2017, by instant  
15 message, defendant NICHOLSON told defendant ALOBA that he was going  
16 to try to buy two iPhones at Best Buy for \$1,900.

17       Overt Act No. 10:       On or about April 30, 2017, by instant  
18 message, defendant NICHOLSON told defendant ALOBA that the purchase  
19 was declined.

20       Overt Act No. 11:       On or about April 30, 2017, by instant  
21 message, defendant ALOBA told defendant NICHOLSON that a \$2,000  
22 purchase was now pre-authorized.

23       Overt Act No. 12:       On or about April 30, 2017, by instant  
24 message, defendant NICHOLSON told defendant ALOBA that the purchase  
25 of the iPhones was declined again.

26       Overt Act No. 13:       On or about April 30, 2017, defendant ALOBA  
27 called American Express about the M.M. American Express card.  
28

1        Overt Act No. 14:    On or about April 30, 2017, at a GameStop in  
2    La Verne, California, defendant NICHOLSON used the M.M. American  
3    Express card to purchase video game consoles, gift cards, and other  
4    items collectively worth approximately \$2,045.

5        Overt Act No. 15:    On or about April 30, 2017, by instant  
6    message, defendant NICHOLSON confirmed to defendant ALOBA that the  
7    M.M. American Express card worked for three transactions for \$698,  
8    \$784, and \$562.

9        Overt Act No. 16:    On or about April 30, 2017, by instant  
10   message, defendant NICHOLSON asked defendant ALOBA for his Bitcoin  
11   address so that he could pay defendant ALOBA his share of the  
12   proceeds.

13    **B. May 4, 2017 Attempted Use of Victim G.F.'s Bank of America**  
14    **Credit Card (Defendants ALOBA and NICHOLSON)**

15        Overt Act No. 17:    On or about May 4, 2017, defendant ALOBA  
16   received three emails in the Realmangreat Account from a phishing  
17   website containing victim G.F.'s PII, email credentials, and credit  
18   card information for G.F.'s Bank of America credit card ending in  
19   4827 (the "G.F. Bank of America card").

20        Overt Act No. 18:    On or about May 4, 2017, by instant message,  
21   defendant ALOBA told defendant NICHOLSON that he had new victim  
22   credit card information and asked if NICHOLSON was ready to use it.

23        Overt Act No. 19:    On or about May 4, 2017, by instant message,  
24   defendant ALOBA sent defendant NICHOLSON victim G.F.'s PII and the  
25   G.F. Bank of America card information.

26        Overt Act No. 20:    On or about May 4, 2017, by instant message,  
27   defendant NICHOLSON sent defendant ALOBA a photo of a Samsung phone  
28



1 on whose screen was displayed options for receiving a digital wallet  
2 verification code.

3 Overt Act No. 21: On or about May 4, 2017, by instant message,  
4 defendant ALOBA told defendant NICHOLSON to choose the email option.

5 Overt Act No. 22: On or about May 4, 2017, by instant message,  
6 defendant ALOBA sent defendant NICHOLSON a verification code.

7 Overt Act No. 23: On or about May 4, 2017, at a Macy's in  
8 Topanga Canyon, defendant NICHOLSON made three attempts to purchase  
9 items collectively worth approximately \$1,735.

10 Overt Act No. 24: On or about May 4, 2017, by instant message,  
11 defendant NICHOLSON told defendant ALOBA that the Macy's purchase was  
12 declined and asked defendant ALOBA to contact the bank.

13 Overt Act No. 25: On or about May 4, 2017, by instant message,  
14 defendant ALOBA told defendant NICHOLSON that the G.F. Bank of  
15 America card was "good" and that he was on the phone with Bank of  
16 America confirming the available balance on the G.F. Bank of America  
17 card.

18 Overt Act No. 26: On or about May 4, 2017, by instant message,  
19 defendant NICHOLSON sent defendant ALOBA a photo of a phone on whose  
20 screen was displayed account information for the G.F. Bank of America  
21 card showing that a charge for approximately \$1,735 had been declined  
22 three times.

23 Overt Act No. 27: On or about May 4, 2017, by instant message,  
24 defendant ALOBA told defendant NICHOLSON that he had called the bank  
25 and learned that the G.F. Bank of America card was no longer working.



1 C. May 31, 2017 Office 365 Phishing Email to Victim M.P.

2 (Defendants ALOBA and ADEDAMOLA)

3 Overt Act No. 28: On an unknown date, defendant ALOBA obtained  
4 the email credentials for victim K's email account,  
5 [victimK]@cox.net.

6 Overt Act No. 29: On or about May 22, 2017, using victim K's  
7 email credentials, defendant ALOBA logged into the [victimK]@cox.net  
8 email account without authorization and sent a test email to himself  
9 at the Yalobaz Account.

10 Overt Act No. 30: On or about May 30, 2017, by instant  
11 message, defendant ALOBA asked defendant ADEDAMOLA to send him the  
12 Office 365 phishing kit.

13 Overt Act No. 31: On or about May 30, 2017, by instant  
14 message, defendant ADEDAMOLA sent defendant ALOBA the Office 365  
15 phishing kit that defendant ADEDAMOLA had encrypted to avoid  
16 detection, and advised defendant ALOBA how to use it.

17 Overt Act No. 32: On or about May 31, 2017, using victim K's  
18 email credentials, defendant ALOBA logged into the [victimK]@cox.net  
19 email account without authorization and sent the Office 365 phishing  
20 email to victim M.P. at her LASC email address.

21 Overt Act No. 33: On or about May 31, 2017, by instant  
22 message, defendant ALOBA confirmed to defendant ADEDAMOLA that  
23 defendant ALOBA was able to send out 8,000 Office 365 phishing  
24 emails.

25 Overt Act No. 34: On or about May 31, 2017, by instant  
26 message, defendant ALOBA sent victim M.P.'s LASC email credentials to  
27 defendant ADEDAMOLA.

1 D. July 21, 2017 Distribution of the Dropbox Phishing Email  
2 (Defendants ALOBA and ALAGBADA)

3 Overt Act No. 35: On or about July 20, 2017, by instant  
4 message, defendant ALAGBADA sent defendant ALOBA a screenshot of a  
5 harvester email account for the Dropbox phishing kit.

6 Overt Act No. 36: On or about July 20, 2017, by instant  
7 message, defendant ALOBA asked defendant ALAGBADA to send the content  
8 of the Dropbox phishing email to the Realmangreat and the Yalobaz  
9 Accounts.

10 Overt Act No. 37: On or about July 21, 2017, by instant  
11 message, defendant ALAGBADA sent defendant ALOBA the Dropbox phishing  
12 kit.

13 Overt Act No. 38: On or about July 21, 2017, by instant  
14 message, defendant ALAGBADA explained to defendant ALOBA how to  
15 access a user's contacts in Office 365.

16 Overt Act No. 39: On or about July 21, 2017, using victim  
17 M.P.'s LASC email credentials, defendant ALOBA logged into the  
18 [victimMP]@lacourts.org email account without authorization.

19 Overt Act No. 40: On or about July 21, 2017, by instant  
20 message, defendant ALOBA told defendant ALAGBADA that defendant ALOBA  
21 had accessed a victim's contacts and was going to send phishing  
22 emails from the victim's mailbox.

23 Overt Act No. 41: On or about July 21, 2017, without  
24 authorization, defendant ALOBA sent the Dropbox phishing email from  
25 [victimMP]@lacourt.org to approximately 550 LASC employees.

1 E. July 24 to 26, 2017 Distribution of the American Express  
2 Phishing Email (Defendants ALOBA and IONICLE)

3 Overt Act No. 42: On or about July 20, 2017, by instant  
4 message, defendant Ionicle sent defendant ALOBA a zip file named  
5 "All\_Pages.zip" that contained approximately 17 phishing kits,  
6 including the American Express phishing kit.

7 Overt Act No. 43: On or about July 21, 2017, in the  
8 Realmangreat Account, defendant ALOBA possessed the LASC email  
9 credentials of approximately 127 LASC employees that had been  
10 harvested from the Dropbox phishing website, including victims R.H.,  
11 R.I., P.N., and M.C.

12 Overt Act No. 44: On or about July 24, 2017, using victim  
13 R.H.'s LASC email credentials, defendant ALOBA logged into the  
14 [victimRH]@lacourts.org email account without authorization.

15 Overt Act No. 45: On or about July 24, 2017, without  
16 authorization, defendant ALOBA sent the American Express phishing  
17 email from [victimRH]@lacourts.org to [victimRF]@uml.edu.

18 Overt Act No. 46: On or about July 24, 2017, without  
19 authorization, defendant ALOBA sent the American Express phishing  
20 email from [victimRH]@lacourts.org to [victimG]@webstationinc.com.

21 Overt Act No. 47: On or about July 24, 2017, without  
22 authorization, defendant ALOBA sent the American Express phishing  
23 email from [victimRH]@lacourts.org to [victimGI]@lgsinnovations.com.

24 Overt Act No. 48: On or about July 24, 2017, using victim  
25 R.I.'s LASC email credentials, defendant ALOBA logged into the  
26 [victimRI]@lacourts.org email account without authorization.



1        Overt Act No. 49:    On or about July 25, 2017, without  
2 authorization, defendant ALOBA sent a test email from  
3 [victimRI]@lacourts.org to himself at the Yalobaz Account.

4        Overt Act No. 50:    On or about July 25, 2017, without  
5 authorization, defendant ALOBA sent the American Express phishing  
6 email from [victimRI]@lacourts.org to himself at the Yalobaz Account.

7        Overt Act No. 51:    On or about July 25, 2017, without  
8 authorization, defendant ALOBA sent the American Express phishing  
9 email from [victimRI]@lacourts.org to [victimAB]@columbia.edu.

10       Overt Act No. 52:    On or about July 25, 2017, without  
11 authorization, defendant ALOBA sent the American Express phishing  
12 email from [victimRI]@lacourts.org to [victimAC]@co.collins.tx.us.

13       Overt Act No. 53:    On or about July 25, 2017, without  
14 authorization, defendant ALOBA sent the American Express phishing  
15 email from [victimRI]@lacourts.org to [victimA]@etonbio.com.

16       Overt Act No. 54:    On or about July 25, 2017, without  
17 authorization, defendant ALOBA sent the American Express phishing  
18 email from [victimRI]@lacourts.org to [victimE]@yahoo.com

19       Overt Act No. 55:    On or about July 24, 2017, using victim  
20 P.N.'s LASC email credentials, defendant ALOBA logged into the  
21 [victimPN]@lacourts.org email account without authorization.

22       Overt Act No. 56:    On or about July 26, 2017, without  
23 authorization, defendant ALOBA sent a test email from  
24 [victimPN]@lacourts.org to himself at the Yalobaz Account.

25       Overt Act No. 57:    On or about July 24, 2017, using victim  
26 M.C.'s LASC email credentials, defendant ALOBA logged into the  
27 [victimMC]@lacourts.org email account without authorization.  
28

1        Overt Act No. 58:    On or about July 26, 2017, without  
2 authorization, defendant ALOBA sent a test email from  
3 [victimMC]@lacourts.org to himself at the Yalobaz Account.

4        Overt Act No. 59:    On or about July 30, 2017, by instant  
5 message, defendant Ionicle demanded payment from defendant ALOBA for  
6 the 17 phishing kits in the "All\_Pages" file.

7        Overt Act No. 60:    On or about August 1, 2017, defendant ALOBA  
8 paid defendant Ionicle in Bitcoin for the 17 phishing kits.

## COUNTS TWO THROUGH SEVENTEEN

[18 U.S.C. §§ 1349, 1343; 2(a)]

9. The Grand Jury repeats, re-alleges, and incorporates by reference the allegations set forth in paragraphs 1-4 and 7 of this First Superseding Indictment as if fully set forth herein.

I. SCHEME TO DEFRAUD

10. Beginning on a date unknown to the Grand Jury and continuing until on or about August 1, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendants ALOBA, ADEDAMOLA, ALAGBADA, "Ionicle," and NICHOLSON, together with others known and unknown to the Grand Jury, each aiding and abetting the other, knowingly and with intent to defraud, devised, participated in, and executed and attempted to execute a scheme to defraud victims as to material matters, and to obtain money and property from such victims by means of material false and fraudulent pretenses, representations, and promises, and the concealment of material facts.

11. The fraudulent scheme was operated and was carried out, in substance, as set forth in paragraph 7 of this First Superseding Indictment.

II. USE OF THE WIRES

12. On or about the following dates, within the Central District of California and elsewhere, defendants ALOBA, ALAGBADA, ADEDAMOLA, Ionicle, and NICHOLSON, and others known and unknown to the Grand Jury, for the purpose of executing and attempting to execute the above-described scheme to defraud, transmitted and caused the transmission of the following items by means of wire communication in interstate and foreign commerce:



COUNT	DATE	DEFENDANTS	ITEM WIRED
TWO	4/30/17	ALOBANICHOLSON	\$734.99 charge on victim M.M.'s American Express card ending in 6000
THREE	4/30/17	ALOBANICHOLSON	\$561.50 charge on victim M.M.'s American Express card ending in 6000
FOUR	4/30/17	ALOBANICHOLSON	\$698.46 charge on victim M.M.'s American Express card ending in 6000
FIVE	5/4/17	ALOBANICHOLSON	Attempted \$1,735.65 charge on victim G.F.'s Bank of America card ending in 4827
SIX	7/21/2017	ALOBAADEDAMOLALAGBADA	Email from [VictimMP]@lacourts.org to [VictimRG]@lacourts.org
SEVEN	7/24/2017	ALOBALAGBADA Ionicle	Email from [victimRH]@lacourts.org to [victimRF]@uml.edu
EIGHT	7/24/2017	ALOBALAGBADA Ionicle	Email from [victimRH]@lacourts.org to [victimG]@webstationinc.com
NINE	7/24/2017	ALOBALAGBADA Ionicle	Email from [victimRH]@lacourts.org to [victimGI]@lgsinnovations.com
TEN	7/25/2017	ALOBALAGBADA	Email from [victimRI]@lacourts.org to yalobaz@yahoo.com
ELEVEN	7/25/2017	ALOBALAGBADA Ionicle	Email from [victimRI]@lacourts.org to yalobaz@yahoo.com
TWELVE	7/25/2017	ALOBALAGBADA Ionicle	Email from [victimRI]@lacourts.org to [victimAB]@columbia.edu
THIRTEEN	7/25/2017	ALOBALAGBADA Ionicle	Email from [victimRI]@lacourts.org to [victimAC]@co.collins.tx.us

1	FOURTEEN	7/25/2017	ALoba ALAGBADA Ionicle	Email from [victimRI]@lacourts.org to [victimA]@etonbio.com
2				
3	FIFTEEN	7/25/2017	ALoba ALAGBADA Ionicle	Email from [victimRI]@lacourts.org to [victimE]@yahoo.com
4				
5	SIXTEEN	7/26/2017	ALoba ALAGBADA	Email from [victimPN]@lacourts.org to yalobaz@yahoo.com
6				
7	SEVENTEEN	7/26/2017	ALoba ALAGBADA	Email from [victimMC]@lacourts.org to yalobaz@yahoo.com
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				

## COUNT EIGHTEEN

[18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I); 2(a)]

On or about July 21, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendants ORİYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007," VICTOR ADEDAMOLA, aka "Legendowski," and RIDWAN ALAGBADA, aka "Mr. Hottie Hottie," each aiding and abetting the other, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally and without authorization caused damage by impairing the integrity and availability of data, a program, a system, and information on a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), that is, the email server(s) of Microsoft Corporation ("Microsoft") hosting the Los Angeles Superior Court email account of victim M.P., thereby causing a loss to Microsoft's email client, the Los Angeles Superior Court, aggregating at least \$5,000 in value during a one-year period beginning on or about July 21, 2017.



## COUNT NINETEEN

[18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i), (ii); 2(a)]

On or about July 21, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendant ORİYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007," and VICTOR ADEDAMOLA, aka "Legendowski," each aiding and abetting the other, intentionally accessed without authorization and in excess of authorization a computer, and thereby obtained information, namely, the contents of, level of access to, and security features associated with the Los Angeles Superior Court email account of victim M.P., from a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), that is, from the email server(s) of Microsoft Corporation, for the purpose of private financial gain and in furtherance of a criminal act, to wit, Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Possession of 15 or More Unauthorized Access Devices, in violation of Title 18, United States Code, Section 1029(a)(3).

## COUNT TWENTY

[18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i), (ii); 2(a)]

On or about July 24, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendant ORİYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007," and RIDWAN ALAGBADA, aka "Mr. Hottie Hottie," each aiding and abetting the other, intentionally accessed without authorization and in excess of authorization a computer, and thereby obtained information, namely, the contents of, level of access to, and security features associated with the Los Angeles Superior Court email account of victim R.H., from a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), that is, from the email server(s) of Microsoft Corporation, for the purpose of private financial gain and in furtherance of a criminal act, to wit, Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Possession of 15 or More Unauthorized Access Devices, in violation of Title 18, United States Code, Section 1029(a)(3).

## COUNT TWENTY-ONE

[18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I); 2(a)]

On or about July 25, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendants ORİYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007," RIDWAN ALAGBADA, aka "Mr. Hottie Hottie," and First Name Unknown ("FNU") Last Name Unknown ("LNU"), aka "Ionicle" ("Ionicle"), each aiding and abetting the other, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally and without authorization caused damage by impairing the integrity and availability of data, a program, a system, and information on a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), that is, the email server(s) of Microsoft Corporation ("Microsoft") hosting the Los Angeles Superior Court email account of victim R.I., thereby causing a loss to Microsoft's email client, the Los Angeles Superior Court, aggregating at least \$5,000 in value during a one-year period beginning on or about July 25, 2017.



## COUNT TWENTY-TWO

[18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i), (ii); 2(a)]

On or about July 25, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendant ORİYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007," and RIDWAN ALAGBADA, aka "Mr. Hottie Hottie," each aiding and abetting the other, intentionally accessed without authorization and in excess of authorization a computer, and thereby obtained information, namely, the contents of, level of access to, and security features associated with the Los Angeles Superior Court email account of victim R.I., from a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), that is, from the email server(s) of Microsoft Corporation, for the purpose of private financial gain and in furtherance of a criminal act, to wit, Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Possession of 15 or More Unauthorized Access Devices, in violation of Title 18, United States Code, Section 1029(a)(3).

## COUNT TWENTY-THREE

[18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i), (ii); 2(a)]

On or about July 26, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendant ORIYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007," and RIDWAN ALAGBADA, aka "Mr. Hottie Hottie," each aiding and abetting the other, intentionally accessed without authorization and in excess of authorization a computer, and thereby obtained information, namely, the contents of, level of access to, and security features associated with the Los Angeles Superior Court email account of victim P.N., from a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), that is, from the email server(s) of Microsoft Corporation, for the purpose of private financial gain and in furtherance of a criminal act, to wit, Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Possession of 15 or More Unauthorized Access Devices, in violation of Title 18, United States Code, Section 1029(a)(3).

## COUNT TWENTY-FOUR

[18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i), (ii); 2(a)]

On or about July 26, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendant ORIYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007," and RIDWAN ALAGBADA, aka "Mr. Hottie Hottie," each aiding and abetting the other, intentionally accessed without authorization and in excess of authorization a computer, and thereby obtained information, namely, the contents of, level of access to, and security features associated with the Los Angeles Superior Court email account of victim M.C., from a protected computer, as that term is defined in Title 18, United States Code, Section 1030(e)(2)(B), that is, from the email server(s) of Microsoft Corporation, for the purpose of private financial gain and in furtherance of a criminal act, to wit, Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Possession of 15 or More Unauthorized Access Devices, in violation of Title 18, United States Code, Section 1029(a)(3).



COUNT TWENTY-FIVE

[18 U.S.C. §§ 1028A(a)(1); 2(a)]

On or about May 4, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendants ORİYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007" ("ALOBÀ"), and ROBERT NICHOLSON, aka "Million\$Menace" ("NICHOLSON"), each aiding and abetting the other, knowingly possessed and used, without lawful authority, a means of identification that defendants ALOBA and NICHOLSON knew belonged to other persons, that is, the name, email username and password of victim G.F., during and in relation to the offense of Attempted Wire Fraud, a felony violation of Title 18, United States Code, Section 1349, as charged in Count Five of this First Superseding Indictment.

## COUNT TWENTY-SIX

[18 U.S.C. §§ 1028A(a)(1); 2(a)]

On or about July 21, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendant ORIYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davidan007" ("ALOBA"), VICTOR ADEDAMOLA, aka "Legendowski" ("ADEDAMOLA"), and RIDWAN ALAGBADA, aka "Mr. Hottie Hottie" ("ALAGBADA"), each aiding and abetting the other, knowingly possessed and used, without lawful authority, a means of identification that defendants ALOBA, ADEDALOMA, and ALAGBADA knew belonged to another person, that is, the name, email username and password of victim M.P., during and in relation to the offense of Wire Fraud, a felony violation of Title 18, United States Code, Section 1343, as charged in Count Six of this First Superseding Indictment.

COUNT TWENTY-SEVEN

[18 U.S.C. §§ 1028A(a)(1); 2(a)]

On or about July 24, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendant ORİYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007" ("ALOBA"), and RIDWAN ALAGBADA, aka "Mr. Hottie Hottie" ("ALAGBADA"), each aiding and abetting the other, knowingly possessed and used, without lawful authority, a means of identification that defendants ALOBA and ALAGBADA knew belonged to another person, that is, the email username and password of victim R.H., during and in relation to the offense of Unauthorized Access to a Protected Computer to Obtain Information, a felony violation of Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i), (ii), as charged in Count Twenty of this First Superseding Indictment.



COUNT TWENTY-EIGHT

[18 U.S.C. §§ 1028A(a)(1); 2(a)]

On or about July 25, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendant ORİYOMI SADIQ ALOBA, also known as ("aka") "D Rwal Me Dontry," aka "davisdan007" ("ALOBA"), RIDWAN ALAGBADA, aka "Mr. Hottie Hottie" ("ALAGBADA"), and First Name Unknown ("FNU") Last Name Unknown ("LNU"), aka "Ionicle" ("Ionicle"), each aiding and abetting the other, knowingly possessed and used, without lawful authority, a means of identification that defendants ALOBA, ALAGBADA, and "Ionicle" knew belonged to another person, that is, the email username and password of victim R.I., during and in relation to the

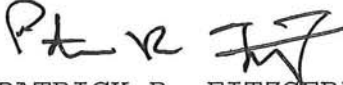
//

1 offense of Unauthorized Impairment of a Protected Computer, a felony  
2 violation of Title 18, United States Code, Section 1030(a)(5)(A),  
3 (c)(4)(B)(i), (c)(4)(A)(i)(I), as charged in Count Twenty-One of this  
4 First Superseding Indictment.

5  
6 A TRUE BILL

7  
8 151  
9 Foreperson

10 NICOLA T. HANNA  
11 United States Attorney

12   
13 PATRICK R. FITZGERALD  
14 Assistant United States Attorney  
15 Chief, National Security Division

16 RYAN WHITE  
17 Assistant United States Attorney  
18 Chief, Cyber & Intellectual Property  
19 Crimes Section

20 JENNIE L. WANG  
21 Assistant United States Attorney  
22 Deputy Chief, Cyber & Intellectual  
23 Property Crimes Section

24 ROBYN K. BACON  
25 Assistant United States Attorney  
26 Cyber & Intellectual Property Crimes  
27 Section  
28